

SpyMax – Mobile Malware On The Frontlines of Syria's Civil War



Agenda

01 Speaker Introduction and Research Purpose

02 SpyMax Overview and Functionality

03 Uncovering Samples & Infrastructure

04 Attribution, Impact, and Conclusion

Research Focus

/Reportage Syria | 14 MIN READ

How a Spyware App Compromised Assad's Army

An investigation reveals how a cyberattack exploited soldiers' vulnerabilities and may have changed the course of the Syrian conflict

Kamal Shahin

Kamal Shahin is a Syrian journalist who worked for decades covering political and social issues

May 26, 2025



Research Methodology

In the early **summer of 2024**, months before the opposition launched Operation Deterrence of Aggression, a mobile application began circulating among a group of Syrian army officers. It carried an innocuous name: **STFD-686**, a string of letters standing for Syria Trust for Development.

A review of the domains associated with **Syr1.store** revealed six linked domains, one of which was registered anonymously. Through SpyMax, whoever was behind the app extracted a devastating range of data from the officers' phones, including their ranks and identities, whether they were responsible for sensitive posts and their geographical locations (possibly in real time). They would have access to troop concentrations, phone conversations, text messages, photos and maps on officers' devices, and be able to monitor military facilities remotely.










app: STFD tag: spymax

Detected

Latest malware on devices

Static analyzed



 STFD-700	 SHA256 d83204a01d3c6f14096f6fe1b59e3f11e8f2c6fb2736792febffb1701fe9a5bc	 Detected	5 months ago
 STFD-752	 SHA256 28fef58c7817926cf7dc0f44e92c1e6716d125b2675e753d415dafa8e7094b37	 Detected	10 months ago
 STFD-686	 SHA256 c82aa80d45022ae7f009e82586e34f990288625c1c876c85e07df74ab3136450	 Detected	a year ago

SpyMax Permissions

- READ_CONTACTS, CALL_LOG, SMS
- ACCESS_COARSE_LOCATION
- RECORD_AUDIO
- CAMERA
- READ_EXTERNAL_STORAGE
- INTERNET
- RECEIVE_BOOT_COMPLETED
- SYSTEM_ALERT_WINDOW



Domain: syr1[.]store
September 2023

**الأمانة
السورية
للتنمية**
Syria Trust for
Development

منظمة غير حكومية وغير هادفة للربح تعمل على دعم واحسان المبادرات المحلية، ويشجع المواطنة النشطة وروح المبادرة والبطوع، وبناء القدرات، وتبادل المعرفة، وإقامة شراكات مع أفراد ومنظمات المجتمع المدني لمناصرة قضايا التنمية، و توسيع مساحة ودور المجتمع المدني في التخطيط وصنع القرار في البلاد.

مشروع جديد للأمانة السورية للتنمية يهدف إلى دعم الأبطال في الجيش العربي السوري الذين يضحون لتجبا سوريا بعرة وكرامة

الأمانة
الاسم الكامل

الأمانة
تاريخ الولادة

الأمانة
محل الولادة

الأمانة
مكان الإقامة الحالي

الأمانة
اللقب الاستثنائية

الأمانة
عدد الأبناء

الأمانة
رقم الهاتف

**SYRIA TRUST FOR
DEVELOPMENT**
بمواصل أمرى عن الماء العذبة

DEVELOPMENT
رابط التوظيف

سوف يتم التواصل معكم من قبل موظف للإستعلامات
يرجى الاحتفاظ بهذا البرنامج على جهازك لمصلحتك اى جديد
للتواصل معنا عبر تطبيق فيسبوك للحالات المستعجلة والإسراع بتقديم المساعدة
وتثبيت الاسم بشكل مباشر
[اضغط هنا](#)

Domain: syr1[.]store
October 2023

الأمانة واحدة

الأمانة السورية للتنمية

Syria Trust for
Development

نتمتع من حكومتنا واهتمامها الفريد بخلق بيئة داعمة وحيوية للمواطنين السوريين ونسعى لتوفير كافة الخدمات والمنتجات التي يحتاجونها في ظل الظروف الصعبة التي يمر بها سوريا. نحن ملتزمون بالشفافية والنزاهة في جميع تعاملاتنا، ونسعى لتقديم أفضل الخدمات والمنتجات التي يحتاجونها في ظل الظروف الصعبة التي يمر بها سوريا. نحن ملتزمون بالشفافية والنزاهة في جميع تعاملاتنا، ونسعى لتقديم أفضل الخدمات والمنتجات التي يحتاجونها في ظل الظروف الصعبة التي يمر بها سوريا.

اسم العائلة

اسم الاب

تاريخ الولادة

00/00/0000

مكان الولادة

مكان الإقامة الحالي

الخطبة الانتمائية

اسم المرحوم

عدد الاولاد

رقم الهاتف

نوع المساعدة المطلوبة

تفاصيل أخرى عن الحالة المالية

زرناك المتطوع

سوف يتم التواصل معك من قبل موظف للإستعلامات
برجى الاحتفاظ بهذا البرنامج على جهازك ليتمكنك اى جديد
للتواصل معنا عبر تطبيق فيسبوك للحالات المستعجلة والإسراع بتقديم المساعدة
وتثبيت الاسم بشكل مأسنر

[اضغط هنا](#)



الأمانة
السورية
للتنمية

Syria Trust for
Development



© 2023 Syria Trust for Development

Domain: syr1[.]online
January 2024

الأمانة السورية للتنمية

**...قدايتي الوطن...
(الغاية)**

تقديم الدعم الكامل لتوفير حياة كريمة لنفق الأطفال على جهات الفئات وتقديم الرعاية اللازمة لهم.
يهدف المشروع إلى تقديم الدعم المالي والمعنوي للعمال السوريين الذين يعانون من الفقر والبطالة، من خلال توفير فرص العمل والتمويل الأصغر، مما يساهم في تحسين مستويات المعيشة وخلق فرص العمل في المناطق الريفية والبلدات النائية. كما يساهم المشروع في تعزيز التنمية البشرية والفنون الريفية ولا يشمل المدنيين.

تقديم العديد من المنح المالية الشهرية لتسهيل الحياة المعيشية للسوريين وجميع أفراد عائلاتهم من خلال ضمان توفير الدخل الكافي للأسر.



بعض نشاطات الأمانة السورية للتنمية بحضرة السيدة الأولى أسماء الأسد



زيارة السيدة الأولى أسماء الأسد لمركز بركاب الأطراف المساندة لمرضى الوطن وتقديم الدعم اللازم لهم ورفع روحهم المعنوية



وقفة السيدة الأولى مع مرضى الوطن في مراكز الأمانة السورية للتنمية لمعالجة مرضى الوطن



زيارة السيدة الأولى أسماء الأسد لمركز بركاب أمه الشهداء ضمن فعاليات الأمانة السورية للتنمية



السيدة الأولى أسماء الأسد تلقي خطاباً في مؤتمر جمعيات الأمانة السورية للتنمية



إتتماع سيادة الرئيس بشار الأسد مع قيادة وعضوات اللجنة العليا لحياطة الملابس الخفيفة وجمع الخطة الهادفة لرفع المعنويات الرعايية للمارحة

يرجى تسجيل بريدك الإلكتروني أو حسابك
 (المستخدم أو البريد الإلكتروني في مشروعنا)

البريد الإلكتروني: info@asat.org.sy
 الهاتف: +963 11 555 5555
 @asat.org.sy

الأمانة السورية للتنمية
 سورية - دمشق

جميع الحقوق محفوظة. الأمانة السورية للتنمية 2023



Domain: syr1[.]online
October 2024

مؤسسته سوريا العد للإغاثة بترحب بكم

بجزة اجنل عة

ممشروع الذعم المالل عن بعد للمحنامل في الذاحل السورل

مؤسسته سورلا العد للإغاثة بآء عملها في محصر عام 2011 وهلم بالخالفة السورلة المواجهه على الأراسل المصربة كما أها عمل على إرسال المساعءاء للمحنامل في الذاحل السورل
مؤسسته خبره بعهوءة باء مءلله بعمى إلى كفاءه و بعهوءة المجمع وهه أفضل الأسس و المامس
بعمل مؤسسته سورلا العد للإغاثة في محالات العمل الأفاةة و التعموره و الطبة و التعللمه بما بعلها بعلل أعلب
الإحناطاب عملها في محصر

أهءاء المؤسسه
مساعءه ورعاةه العناة الأكم مساعءه و بعهوءه سبل بكمهم إهمالها
بفعم الذعم المادل والممس للمحنامل
بفعم جماء الرعاة الأجماعه للأشخاص بوق الأعاةه

الاسم النلاسل

اسم الام

نارلح الولاءه

مكان الولاءه

مكان الإقامه الحالل

الحالة الأجماعه

اسم الروجه

عءر الأولاء

رقم الهاف

بوع المساعءه الموقوفه

بفاصل أحرى عن الحالة المادبه

ببءاءة

سوف بكم البواصل بكم من فمل موفف للإسبعلاماء
ببوحى الإحناط بهءا البرامح على مءارك بسلكم أن بءب

Domain: syr1[.]online
December 2024 (Post War)



Благотворительная организация Мосфарм
مشروع الدعم المالي عن بعد للمحتاجين في الداخل السوري

Наша организация является гуманитарной благотворительной организацией, целью которой является поддержка дружественного России сирийского народа деньгами, едой и медицинской помощью. Мы желаем всего наилучшего раненому и стойкому сирийскому народу перед лицом терроризма.
منظمتنا هي منظمة خيرية إنسانية هدفها دعم الشعب السوري الصديق أرمينا بالمال و الغذاء و الطمأنينة وتمنيت كل الخير للشعب السوري الحريج و الصامد بوجه الإرهاب
. مؤسسة خيرية نموذج ذات طابع مدني يسهم إلى كفاية و تنمية المجتمع وفق أفضل الأسس و المعايير

أهداف المؤسسة
مساعدة ورعاية الفئات الأكثر هشاشة وتوفير سبل تكفيهم إقتصاديا
تقديم الدعم المادي والمعنوي للمحتاجين
تقديم خدمات الرعاية الاجتماعية للأشخاص ذوي الإعاقة

الاسم الثلاثي

اسم الام

تاريخ الولادة

مكان الولادة

مكان الإقامة الحالي

الحالة الاجتماعية

اسم الزوجة

عدد الاولاد

رقم الهاتف

نوع المساعدة المتوقعة

تفاصيل أخرى عن الحالة المادية

[إرسال البيانات](#)

ننوه بتم التواصل معكم من قبل موظف للاستعلامات
برحمتي الاحتفاظ بهذا البرنامج على جهازك لتتمكن ان جديد

Domain: syr1[.]online
July 2025 (Post War)

رابطه العلوين السوريين في أوروبا

جميعا إنسانية التضامنة جديدة نهر ربحه
نعم جمع فوات الثقافة العنوية المنص من أوروبا
من أجل تحقيق الأضاح الإنسانية المشتركة

THE ASSOCIATION OF SYRIAN REFUGEES IN EUROPE
رابطه العلوين السوريين في أوروبا

طلب دعم مادي

الاسم الثلاثي:

اسم الأم:

رقم الهاتف:

مكان الإقامة الحالي:

الحالة الاجتماعية:
- اخر -

عدد الأولاد:

نوع المساعدة المطلوبة:

يرجى الاحتفاظ بهذا التطبيق على هاتفك سيتم تزويدك بأسعارات الجواله عليه و لنوافيكم بكل جديد

Image: Sept 2015 © DomainTools.com

الأمانة السورية للتنمية
Syria Trust for Development

من نحن ▾ أتر عملنا ▾ المكتبة الإعلامية ▾ الأخبار ▾ انضم إلى فريقنا ▾ دعوة للمشاركة ▾ تواصل معنا

تسجيل الدخول

الرئيسية / حساب المستخدم / تسجيل الدخول

في حال كنت لا تملك حساب يمكنك تسجيل حساب جديد

البريد الإلكتروني
كلمة السر

تذكرني

هل نسيت كلمة السر؟

عن الأمانة
تواصل معنا
انضم إلى فريقنا

العلامة البريجه
انضم لحملتك آخر الأخبار وأحدث النشاطات عبر بريدك الإلكتروني

دمشق، باب شرقي، جادة محمد زهير شميس الحدين
(963*) - 11-4731300
info@syriatrustsy

الأمانة السورية للتنمية
Syria Trust for Development

جميع الحقوق محفوظة - الأمانة السورية للتنمية 2021

About SpyMax

What it is:

- Derived from SpyNote malware
- Features a highly obfuscated code base

How it spreads and communicates:

- Distributed via Telegram channels and phishing sites
- Uses hardcoded servers for command and control

How it operates:

- Prompts users to grant multiple app permissions
- Harvests sensitive data through a webview interface once permissions are granted
- Exfiltrated data via direct socket communication

Spy Family History

Origins:

- SpyNote first released in 2016
- SpyNote previously used by Syria-nexus adversary DEADEYE HAWK


Evolution of variants:

- 2019-2020: **SpyMax** appears in criminal forums
- Additional variants such as CraxsRAT and EagleSpy emerge in 2025

Current landscape:

- CraxsRAT and EagleSpy are the most active variants across current cyber criminal forums
- Detection rules frequently cross-match variants due to shared code base and functionality

Attribution



HOSTINGER

Artık Hazırsınız!

Şimdi tek yapmanız gereken web sitesi dosyalarınızı yüklemek ve yolculuğunuza başlamak. Nasıl yapacağınızı aşağıdan kontrol ediniz:

[Web sitemi Hostinger'a nasıl taşıyabilirim?](#)

[Otomatik Yükleyci ile WordPress nasıl kurulum?](#)

Image Sourced By DepositPhotos.com

Certificate Subject

Distinguished Name	C:rb, CN:Benim ismim, L:Antan, O:Benim Firmam, ST:SANANE, OU:Benim Firmam, email:sahte@gmail.com
Email	sahte@gmail.com
Common Name	Benim ismim
Organization	Benim Firmam
Organizational Unit	Benim Firmam
Country Code	rb
State	SANANE
Locality	Antan

Possible Impacts

- Real-time mapping of deployments
- Location of critical military assets (weapons, comms, facilities)
- Exposed command structure
- Troop movements
- Estimated thousands of affected personnel (according to NewsLine)

Intelligence Gaps

- Attribution is currently **unclear**
- The way in which SpyMax first began circulating among Syrian Army Officers is unknown
- Whether the campaign extends past the samples and infrastructure identified is unknown
- How was the information uploaded to the harvesting webview pages used?

This was not:

- A carefully crafted exploit
- Expensive, stealthy, no-click spyware
- A Zero day

This was:

- Commodity malware that **anyone** can buy



IoCs

C2 Domains:

- west2.shop

WebView Domains:

- syr1[.]store
- syr1[.]online

SHA256 Hashes

- d83204a01d3c6f14096f6fe1b59e3f11e8f2c6fb2736792febffb1701fe9a5bc
- 28fef58c7817926cf7dc0f44e92c1e6716d125b2675e753d415dafa8e7094b37
- c82aa80d45022ae7f009e82586e34f990288625c1c876c85e07df74ab3136450
- 60ca970a774c5ff1ada52170857989721158064b932e999714bff7f4bd8b570c
- db041da97c1f30a6fc7765994b556839f8550774af1662ae0ab105e2fc324487
- 2c1aa8139f55b6566ff8fcb88efccd169040b8cff932683e8d4e1401f9c64644





Questions?



Thank you!